UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,952	12/11/2000	Aravind Sitaraman	CISCO-3294	4939

7590 09/26/2007

David B. Ritchie
Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640

EXAMINER	
PATEL, ASHOKKUMAR B	
ART UNIT	PAPER NUMBER
2154	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/734,952	SITARAMAN ET AL.	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) *1,10-12,21-23,32-35,44 and 45* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-9.13-20.24-31 and 36-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/29/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 are subject to examination. Claims 1, 10-12, 21-23, 32-35, 44 and 45 have been cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/29/2006 has been entered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-9, 13-20 and 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (hereinafter Malan) (US 2002/0035698 A1) in view of Denial of Service Protection The Nozzle by Elizabeth Strother, dated August 20, 2000. (hereinafter Strother).

Referring to claim 2,

Malan teaches a method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers (para. [0064], "Protecting Web (Hypertext Transfer Protocol, or HTTP) services is one specific application of the DoS scrubber. When scrubbing HTTP traffic, the DoS scrubber separates legitimate from malicious Web requests."), the method comprising:

receiving a HTTP request from a subscriber having an established connection (para. [0066] "The DoS scrubber's forwarding engine serves both as an enforcement mechanism and statistics generator. When Internet Protocol (IP) packets enter the scrubber, they are given to the forwarding engine. Upon receipt, the FE determines if the packets belong to an old request, or are part of a new request. If the request is new, a variety of safeguards remove many of the common types of denial of service--such as TCP SYN floods. However, the safeguards also include checking to see if requesting client has been determined malicious by the analysis engine. If so, the request is dealt with in a policy configured manner. For example, if the service is not overwhelmed, it may allow the request to happen; however it can be throttled back using a custom rate limiter.") over a first communication network (Fig. 1, element "INTERNET", para. [0063] "FIG. 1 shows an example use of the DoS scrubber. It depicts a network server providing a publicly accessible service--a public Web server for example. The DoS scrubber is interposed between the server and the Internet.") coupled to at least one other communication network (para. [0063] "FIG. 1 shows an example use of the DoS scrubber. It depicts a network server providing a publicly accessible service--a public Web server for example. The DoS scrubber is interposed

between the server and the Internet.", Fig. 1 showing the network within which "INTERNET SERVER" is located is at least one other communication network. Also note in para. [0051], "The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and enterprise networks.", and para.[0065] "FIG. 2 denotes the denial of service scrubber's high-level architecture. It is comprised of two primary components: the forwarding and the analysis engines. The forwarding engine (FE) has two main responsibilities: applying filtering and rate limiting to sets of Internet hosts, and generating request statistics. The analysis engine (AE) is responsible for the collection and subsequent data mining of the forwarding engine's statistics. Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests."), said request including a Universal Resource Locator (URL) (para. [0064] "Protecting Web (Hypertext Transfer Protocol, or HTTP) services is one specific application of the DoS scrubber;.."");

receiving a profile for said subscriber (para. [0026] "One or more user profiles may be generated from the network traffic and wherein the step of analyzing may include the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user." para. [0027] "The step of generating the one or more user profiles may include the step of generating request statistics for the user from the network traffic.[0028] The request statistics may include connection statistics and service request distributions.");

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile (para. [0065] "Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests.")

Malan teaches "a HTTP GET request" as well as TCP SYN at [0066] "Upon receipt, the FE determines if the packets belong to an old request, or are part of a new request. If the request is new, a variety of safeguards remove many of the common types of denial of service--such as TCP SYN floods. " "Examples of these statistics include: [0067] Size: the request and subsequent reply's size, both in bytes and packets. [0068] Request payload: content of the request at the application layer (e.g., HTTP GET string).

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request. (para. [0066] "However, the safeguards also include checking to see if requesting client has been determined malicious by the analysis engine. If so, the request is dealt with in a policy configured manner. For example, if the service is not overwhelmed, it may allow the request to happen; however it can be throttled back using a custom rate limiter.")

Note: Malan teaches preventing a denial of service attack of an established , that is a HTTP GET request, as well as new connections TCP SYN packet by DoS scrubber through manners of either filtering the requests completely or throttling back their access requests **using a custom rate limiter.** (para, [0063] "..the DoS scrubber can identify malicious users of the service and either filter completely or throttle back

their access.", [0064], "Clients with profiles that are flagged as anomalous are then candidates for their subsequent requests to be attenuated or completely filtered.", [0065], "Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests.")

Malan fails to disclose **custom rate limiter** (filter) detail including said filtering including:

updating a client request count; and

applying server denial of service attack preventative measures when a client request frequency based on said client request count exceeds a maximum request frequency.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, said filtering including:

updating a client request count (page 38, Right Column, lines 4-7, "Our data structure is actually a queue and a buffer. ..... ordered by timestamp... Note: This is inherent to have updating the count.) when said request for said URL is a HTTP GET request (page 39, Right Column, lines, 6-11, Ring 3 of Fig. 5, ".. HTTP get request."); and

applying server denial of service attack preventative measures when a client request frequency based on said client request count exceeds a maximum request frequency. (page 37, Right Column, 35- page 38, Left Column, line 2.)

Thus, Strother teaches "rate limiter" filter to "update a client HTTP request count, and applying HTTP server denial of service attack preventative measures when a client

HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency.

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter to "update a client HTTP request count and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency" as taught by Strother as **"a custom rate limiter" of Malan.**

Using the known technique for updating a client HTTP request count; and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency" to provide the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 3,

Keeping in mind the teachings of Malan as stated above for claim 1, Malan does not teach the method of claim 2, wherein said applying further comprises setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and wherein said applying further comprises setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency. (page 37, Right Column, 35- page 38, Left Column, line 2.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter wherein said applying further comprises setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency as taught by Strother as **"a custom rate limiter" of Malan.**

Using the known technique for setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 4,

Malan teaches "an Internet Service Provider (ISP) associated with said subscriber (Abstract, para. [0023], [0051]), however fails to teach the method of claim 3, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and sending said alarm (page 37, Right Column, 35- page 38, Left Column, line 2.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for sending alarm as taught by Strother as **"a custom rate limiter" of Malan** to an Internet Service Provider (ISP) associated with said subscriber.

Using the known technique for sending said alarm and employing it to send the alarm to an Internet Service Provider (ISP) in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 5,

Malan teaches the method wherein said applying further comprises dropping the data packet containing said request at para.[0063], and [0064], "completely filtered" based on " the service request distribution and packet statistics", however, fails to teach "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "dropping" the requests "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "dropping" the requests "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 6,

Malan teaches the method of claim 2, wherein said applying further comprises shutting down the account used to access said first communication network at para.[0063], and [0064], "completely filtered" based on " the service request distribution

and packet statistics", however, fails to teach "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 7,

Malan teaches the method of claim 6, wherein said applying further comprises disabling HTTP requests for a hold-down period at para.[0063], and [0064], "completely filtered" based on " the service request distribution and packet statistics", however, fails to teach "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "disabling HTTP requests for a hold-down period" " "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 8,

Malan teaches The method of claim 7, further comprising increasing said hold-down period each time at para.[0063], and [0064], "completely filtered" or "throttle back their access" based on " the service request distribution and packet statistics", however, fails to teach "The method of claim 7, further comprising "increasing said hold-down period each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "increasing said hold-down period each time" "when said client HTTP request frequency

exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "increasing said hold-down period each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "increasing said hold-down period each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 9,

Malan teaches The method of claim 8, wherein said hold-down period increases exponentially each time at para.[0063], and [0064], "completely filtered" or "throttle back their access" based on " the service request distribution and packet statistics", however, fails to teach "The method of claim 7, further comprising " The method of claim 8, wherein said hold-down period increases exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "The method of claim 8, wherein said hold-down period increases exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "increasing the hold down period exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "increasing the hold down period exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 13,

Claim 13 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 2. Therefore, claim 13 is rejected for the reasons set forth for the claim 2.

Referring to claim 14,

Claim 14 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 3. Therefore, claim 14 is rejected for the reasons set forth for the claim 3.

Referring to claim 15,

Claim 15 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of

method of claim 4. Therefore, claim 15 is rejected for the reasons set forth for the claim 4.

Referring to claim 16,

Claim 16 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 5. Therefore, claim 16 is rejected for the reasons set forth for the claim 5.

Referring to claim 17,

Claim 17 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 6. Therefore, claim 17 is rejected for the reasons set forth for the claim 6.

Referring to claim 18,

Claim 18 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 7. Therefore, claim 18 is rejected for the reasons set forth for the claim 7.

Referring to claim 19,

Claim 19 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 8. Therefore, claim 19 is rejected for the reasons set forth for the claim 8.

Referring to claim 20,

Claim 20 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 9. Therefore, claim 20 is rejected for the reasons set forth for the claim 9.

Referring to claim 24,

Claim 24 is a claim to an apparatus carrying out the method of claim 2. Therefore, claim 24 is rejected for the reasons set forth for the claim 2.

Referring to claim 25,

Claim 25 is a claim to an apparatus carrying out the method of claim 3. Therefore, claim 25 is rejected for the reasons set forth for the claim 3.

Referring to claim 26,

Claim 26 is a claim to an apparatus carrying out the method of claim 4. Therefore, claim 26 is rejected for the reasons set forth for the claim 4.

Referring to claim 27,

Claim 27 is a claim to an apparatus carrying out the method of claim 5. Therefore, claim 27 is rejected for the reasons set forth for the claim 5.

Referring to claim 28,

Claim 28 is a claim to an apparatus carrying out the method of claim 6. Therefore, claim 28 is rejected for the reasons set forth for the claim 6.

Referring to claim 29,

Claim 29 is a claim to an apparatus carrying out the method of claim 7. Therefore, claim 29 is rejected for the reasons set forth for the claim 7.

Referring to claim 30,

Claim 30 is a claim to an apparatus carrying out the method of claim 8. Therefore, claim 30 is rejected for the reasons set forth for the claim 8.

Referring to claim 31,

Claim 31 is a claim to an apparatus carrying out the method of claim 9. Therefore, claim 31 is rejected for the reasons set forth for the claim 9.

5. Claims 36-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (hereinafter Malan) (US 2002/0035698 A1) in view of Denial of Service Protection The Nozzle by Elizabeth Strother, dated August 20, 2000. (hereinafter Strother) and further in view of Dynarski et al. (hereinafter Dynarski), (US 6, 628, 671).

Referring to claim 36,

Malan teaches an apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, said apparatus comprising: (para. [0064], "Protecting Web (Hypertext Transfer Protocol, or HTTP) services is one specific application of the DoS scrubber. When scrubbing HTTP traffic, the DoS scrubber separates legitimate from malicious Web requests."), the method comprising:

a first receiving interface capable of accepting a HTTP request received from a subscriber, (para. [0066] "The DoS scrubber's forwarding engine serves both as an enforcement mechanism and statistics generator. When Internet Protocol (IP) packets enter the scrubber, they are given to the forwarding engine. Upon receipt, the FE

determines if the packets belong to an old request, or are part of a new request. If the request is new, a variety of safeguards remove many of the common types of denial of service--such as TCP SYN floods. However, the safeguards also include checking to see if requesting client has been determined malicious by the analysis engine. If so, the request is dealt with in a policy configured manner. For example, if the service is not overwhelmed, it may allow the request to happen; however it can be throttled back using a custom rate limiter.") having an established connection originating from a first communication network (Fig. 1, element "INTERNET", para. [0063] "FIG. 1 shows an example use of the DoS scrubber. It depicts a network server providing a publicly accessible service--a public Web server for example. The DoS scrubber is interposed between the server and the Internet." Also note in para. [0051], "The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and enterprise networks.", and para.[0065] "FIG. 2 denotes the denial of service scrubber's high-level architecture. It is comprised of two primary components: the forwarding and the analysis engines. The forwarding engine (FE) has two main responsibilities: applying filtering and rate limiting to sets of Internet hosts, and generating request statistics. The analysis engine (AE) is responsible for the collection and subsequent data mining of the forwarding engine's statistics. Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests."), request including a Universal Resource Locator (URL) (para. [0064]

"Protecting Web (Hypertext Transfer Protocol, or HTTP) services is one specific application of the DoS scrubber.");

a profile request generator capable of generating a profile request based upon said HTTP request; a second receiving interface capable of accepting a requested profile; (para. [0026] "One or more user profiles may be generated from the network traffic and wherein the step of analyzing may include the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user." para. [0027] "The step of generating the one or more user profiles may include the step of generating request statistics for the user from the network traffic.[0028] The request statistics may include connection statistics and service request distributions.");

a filter capable of determining whether said HTTP request is authorized based upon said requested profile, said filter including: (para. [0065] "Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests.")

Malan teaches "a HTTP GET request" as well as TCP SYN at [0066] "Upon receipt, the FE determines if the packets belong to an old request, or are part of a new request. If the request is new, a variety of safeguards remove many of the common types of denial of service--such as TCP SYN floods. " "Examples of these statistics include: [0067] Size: the request and subsequent reply's size, both in bytes and packets. [0068] Request payload: content of the request at the application layer (e.g., HTTP GET string).

an authorizer capable of allowing said HTTP request to be forwarded on at least one other communication network coupled to said first communication network (para. [0026] "One or more user profiles may be generated from the network traffic and wherein the step of analyzing may include the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user." para. [0027] "The step of generating the one or more user profiles may include the step of generating request statistics for the user from the network traffic.[0028] The request statistics may include connection statistics and service request distributions.");; and

a second forwarding interface capable of forwarding said HTTP request on said at least one other communication network. (para. [0066] "However, the safeguards also include checking to see if requesting client has been determined malicious by the analysis engine. If so, the request is dealt with in a policy configured manner. For example, if the service is not overwhelmed, it may allow the request to happen; however it can be throttled back using a custom rate limiter.")

Note: Malan teaches preventing a denial of service attack of an established , that is a HTTP GET request, as well as new connections TCP SYN packet by DoS scrubber through manners of either filtering the requests completely or throttling back their access requests **using a custom rate limiter.** (para, [0063] "..the DoS scrubber can identify malicious users of the service and either filter completely or throttle back their access.", [0064], "Clients with profiles that are flagged as anomalous are then candidates for their subsequent requests to be attenuated or completely filtered.",

[0065], "Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests.")

Malan fails to disclose custom rate limiter (filter) detail including said filtering including:

an updater to update a client request count ;

updating a client request count; and

a responder to apply denial of service attack preventative measures when a client request frequency based on said client request count exceeds a maximum request frequency.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, said filtering including:

updating a client request count (page 38, Right Column, lines 4-7, "Our data structure is actually a queue and a buffer. ..... ordered by timestamp... Note: This is inherent to have updating the count.) when said request for said URL is a HTTP GET request (page 39, Right Column, lines, 6-11, Ring 3 of Fig. 5, ".. HTTP get request."); and

a responder to apply server denial of service attack preventative measures when a client request frequency based on said client request count exceeds a maximum request frequency. (page 37, Right Column, 35- page 38, Left Column, line 2.)

Thus, Strother teaches "rate limiter" filter to "update a client HTTP request count, and applying HTTP server denial of service attack preventative measures when a client

HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency.

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter to "update a client HTTP request count and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency" as taught by Strother as **"a custom rate limiter" of Malan.**

Using the known technique for updating a client HTTP request count; and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency" to provide the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Both, Malan as well as Strother fail to teach "a first forwarding interface capable of sending said profile request to an Authentication, Authorization, and Accounting (AAA) server."

Malan teaches a profile request generator capable of generating a profile request based upon said HTTP request; a second receiving interface capable of accepting a requested profile; (para. [0026] "One or more user profiles may be generated from the network traffic and wherein the step of analyzing may include the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user." para. [0027] "The step of generating the one or more user profiles may include

the step of generating request statistics for the user from the network traffic.[0028] The request statistics may include connection statistics and service request distributions.") with having the profile locally available.

Dynarski teaches a first forwarding interface capable of sending said profile request to an Authentication, Authorization, and Accounting (AAA) server". (col. 6, line 36-39, "The authentication server 28, in a preferred embodiment, comprises a general purpose computer functioning as a RADIUS server (a known device) providing accounting, authorization and authentication functions for a plurality of mobile users.")

Therefore it would have been obvious to one of ordinary skills in the art to employ Authentication, Authorization, and Accounting (AAA) server of Dynarski replacing the profile generator of Malan, that is substituting one method for the other to achieve the predictable result of extracting the user profile from Authentication, Authorization, and Accounting (AAA) server

Referring to claim 37,

Keeping in mind the teachings of Malan as stated above for claim 36, Malan does not teach the apparatus of claim 36, wherein said responder further sets an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and sets an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency. (page 37, Right Column, 35- page 38, Left Column, line 2.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter wherein said applying further comprises setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency as taught by Strother as **"a custom rate limiter" of Malan.**

Using the known technique for setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 38,

Malan teaches "an Internet Service Provider (ISP) associated with said subscriber (Abstract, para. [0023], [0051]), however fails to teach The apparatus of claim 37, wherein said responder sends said alarm to an Internet Service Provider (ISP) associated with said subscriber.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and sends said alarm (page 37, Right Column, 35- page 38, Left Column, line 2.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for sending alarm as taught by Strother as **"a custom rate limiter" of Malan** to an Internet Service Provider (ISP) associated with said subscriber.

Using the known technique for sending said alarm and employing it to send the alarm to an Internet Service Provider (ISP) in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 39,

Malan teaches responder dropping the data packet containing said request at para.[0063], and [0064], "completely filtered" based on " the service request distribution and packet statistics", however, fails to teach "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it "dropping" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 40,

Malan teaches the method of claim 36, apparatus of claim 36, wherein said responder shuts down the account used to access said first communication network (para.[0063], and [0064], "completely filtered" based on " the service request distribution

and packet statistics", however, fails to teach "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it for "shutting down the account" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 41,

Malan teaches the apparatus of claim 40, wherein said responder disables HTTP requests for a hold-down period at para.[0063], and [0064], "completely filtered" based on " the service request distribution and packet statistics", however, fails to teach "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter for "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**"

Using the known technique for sending said alarm and employing it for "disabling HTTP requests for a hold-down period" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 42,

Malan teaches The apparatus of claim 41, wherein said responder increases said hold-down period each time at para.[0063], and [0064], "completely filtered" or "throttle back their access" based on " the service request distribution and packet statistics", however, fails to teach wherein said responder increases said hold-down period each time "said client HTTP request frequency exceeds said maximum HTTP request frequency.

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "increasing said hold-down period each time" "when said client HTTP request frequency

exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35-page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter to "increase said hold-down period each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it to "increase said hold-down period each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

Referring to claim 43,

Malan teaches apparatus of claim 42, wherein said responder increases said hold-down period at para.[0063], and [0064], "completely filtered" or "throttle back their access" based on " the service request distribution and packet statistics", however, fails to teach "each time said client HTTP request frequency exceeds said maximum HTTP request frequency. , wherein said responder increases said hold-down period exponentially each time said client HTTP request frequency exceeds said maximum HTTP request frequency."

Strother teaches "The Nozzle" in Fig. 4, page 38 in the form of filtering, and "The apparatus, wherein said hold-down period increases exponentially each time" "when

said client HTTP request frequency exceeds said maximum HTTP request frequency." (page 37, Right Column, line 35- page 38, Left Column, line 6.)

Therefore it would have been obvious to one of ordinary skills in the art to employ "rate limiter" filter to "increase hold-down period exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." as taught by Strother in **"a custom rate limiter" of Malan.**

Using the known technique for sending said alarm and employing it to "increase hold-down period exponentially each time" "when said client HTTP request frequency exceeds said maximum HTTP request frequency." in the rate limiting mechanism as desired in the DoS Scrubber (Fig. 1, element "DoS Scrubber" and Fig. 2) of Malan would have been obvious to one of ordinary skill.

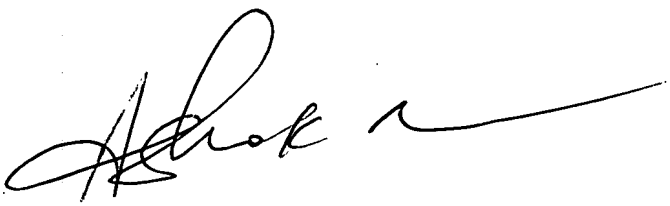
Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 6:30 am-4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan A. Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ashok Patel
Examiner
AU 2154